



## UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,495	11/27/2001	Doug Rollins	M4065.0486/P486	8165
24998	7590	02/18/2009	EXAMINER	
DICKSTEIN SHAPIRO LLP			GELAGAY, SHIWAYE	
1825 EYE STREET NW			ART UNIT	PAPER NUMBER
Washington, DC 20006-5403			2437	
MAIL DATE		DELIVERY MODE		
02/18/2009		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 09/993,495	<b>Applicant(s)</b> ROLLINS, DOUG
	<b>Examiner</b> SHEWAYE GELAGAY	<b>Art Unit</b> 2437

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If no period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(o).

#### Status

1) Responsive to communication(s) filed on 12 November 2008.

2a) This action is FINAL.      2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-12 and 14-26 is/are pending in the application.

4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5) Claim(s) \_\_\_\_\_ is/are allowed.

6) Claim(s) 1-12 and 14-26 is/are rejected.

7) Claim(s) \_\_\_\_\_ is/are objected to.

8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO/SB/08)  
 Paper No(s)/Mail Date \_\_\_\_\_

4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date \_\_\_\_\_

5) Notice of Informal Patent Application  
 6) Other: \_\_\_\_\_

**DETAILED ACTION**

1. This Office Action is in response to Applicants amendment filed on November 12, 2008. Claim 1 has been amended. Claims 1-12 and 14-26 are pending.

***Response to Amendment***

2. The Declaration filed on 11/12/08 under 37 CFR 1.131 is sufficient to overcome the Serceki et al. (U.S. 2003/0078072) reference.

***Response to Arguments***

3. Applicant's arguments filed November 12, 2008 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1, 6-8, 14-20 and 26 rejected under 35 U.S.C. 103(a) as being unpatentable over Morimoto US 7,024,553 in view of Spies et al. (hereinafter Spies) US 6,055,314.

As per claim 1:

Morimoto teaches a method of updating and using an encryption key used by a wireless station for encrypted communications with a wired portion of the network, said method comprising:

connecting to a key updating device which is connected to a wired portion of said network said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device; (col. 7, lines 51-67; col. 8, lines 25-61)

connecting a network communications device to an encryption key updating device which is connected to a wired portion of said network said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device; (col. 7, lines 51-67; col. 8, lines 25-61)

replacing an existing encryption key in said network communications device with a new encryption key from said generator sent over said wired portion of said network; (col. 7, lines 51-67; col. 8, lines 25-61)

reconnecting said network communications device containing said new encryption key with said wireless station of said network. (col. 7, lines 51-67; col. 8, lines 25-61) and

accessing said new encryption key during an encrypted communication. (col. 7, lines 51-67; col. 8, lines 25-61)

Morimoto does not explicitly physically separating a wireless network device and physically reconnecting the wireless communication device from a wireless station. Spies in analogous art, however, discloses accessing a new encryption key on said

Art Unit: 2437

network device during an encrypted communication. (col. 6, lines 10-32) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Morimoto with Spies in order to implement decryption capabilities on the IC card without exposing the decryption capabilities, thereby providing secure delivery system that permits easy replacement of security protocol. (Abstract; col. 2, lines 16-18; Spies)

As per claims 6-7, 14, 16 and 26:

The combination of Morimoto and Spies teaches all the subject matter as discussed above. In addition, Spies further discloses a method wherein said network communications device is configured on a plug-in card and is physically connection to said network by inserting said network communications device into a card tray at said updating device. (col. 6, lines 10-32)

As per claims 8 and 15:

Morimoto teaches a network comprising:

a wired station connected to a wired network, (col. 7, lines 51-67; col. 8, lines 25-61) said wired station comprising:

an encryption key generator for generating an encryption key; (col. 7, lines 51-67; col. 8, lines 25-61)

a network communication device for transmitting said encryption key over said wired network; (col. 7, lines 51-67; col. 8, lines 25-61) and

a wired encryption key updating device connected to said wired network; (col. 7, lines 51-67; col. 8, lines 25-61)

a wireless station configured to be wirelessly connected to said network and to communicate with said wired network through communications encrypted with an encryption key, (col. 7, lines 51-67; col. 8, lines 25-61) said wireless station comprising:

a wireless network communication device containing an encryption key, being disconnectable from said wireless station and connectable said wired encryption key updating device wired to said network to receive, store and use a new encryption key which is configured to be transmitted over said wired network by said wired network communications device. (col. 7, lines 51-67; col. 8, lines 25-61)

Morimoto does not explicitly disclose a wireless network device being physically disconnectable from the wireless station and physically connectable to said wired encryption updating device. Spies in analogous art, however, discloses a wireless network device being physically disconnectable from the wireless station and physically connectable to said wired encryption updating device. (col. 6, lines 10-32) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Morimoto with Spies in order to implement decryption capabilities on the IC card without exposing the decryption capabilities, thereby providing secure delivery system that permits easy replacement of security protocol. (Abstract; col. 2, lines 16-18; Spies)

As per claim 17:

Morimoto teaches a wireless network communications device comprising:

A removable wireless communications network card adapted to be connected to and disconnected from a wireless station card interface; (col. 7, lines 51-67; col. 8, lines 25-61)

a storage area said network card which stores an updateable encryption key for use in conducting encrypted wireless network communications, (col. 7, lines 51-67; col. 8, lines 25-61) said encryption key being updateable when said card is connected to a wired network card interface which supplies a new encryption key. (col. 7, lines 51-67; col. 8, lines 25-61)

Morimoto does not explicitly disclose a wireless network device being physically connected to a wired network card interface which supplies a new encryption key. Spies in analogous art, however, discloses a wireless network device being physically connected to a wired network card interface which supplies a new encryption key. (col. 6, lines 10-32) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Morimoto with Spies in order to implement decryption capabilities on the IC card without exposing the decryption capabilities, thereby providing secure delivery system that permits easy replacement of security protocol. (Abstract; col. 2, lines 16-18; Spies)

As per claims 18 and 19:

The combination of Morimoto and Spies teaches all the subject matter as discussed above. In addition, Spies further discloses a method wherein card interface for providing a new encryption key is a PCMCIA card interface. (col. 6, lines 10-32)

As per claim 20:

Morimoto teaches an encryption key programming system comprising:  
an encryption key generator connected to a wired network; (col. 7, lines 51-67;  
col. 8, lines 25-61)

a programming device connected to said wired network for receiving over a wire connection an encryption key from said generator, said programming device being adapted to receive a wireless network communications device containing an updatable encryption key and storing said received encryption key in said wireless network communications device. (col. 7, lines 51-67; col. 8, lines 25-61)

Morimoto does not explicitly disclose a programming device adapted to physically receive a wireless network communications device Spies in analogous art, however, discloses a wireless network device being physically connected to a wired network card interface which supplies a new encryption key. (col. 6, lines 10-32)  
Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Morimoto with Spies in order to implement decryption capabilities on the IC card without exposing the decryption capabilities, thereby providing secure delivery system that permits easy replacement of security protocol. (Abstract; col. 2, lines 16-18; Spies)

3. Claims 2-3, 9-10 and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morimoto US 7,024,553 in view of Spies et al. (hereinafter Spies) US 6,055,314 and in view of Campbell, Jr. U.S. Patent 4,369,332.

As per claims 2-3, 9-10 and 21-23:

The combination of Morimoto and Spies teaches all the subject matter as discussed above. Both references do not explicitly disclose a method wherein said new encryption key is generated at user-defined intervals or on user-specified days. Campbell in analogous art, however, discloses a method wherein said new encryption key is generated at user-defined intervals or on user-specified days. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Morimoto and Spies with Campbell Spies in order to implement decryption capabilities on the IC card without exposing the decryption capabilities. (Abstract; Spies)

4. Claims 4-5, 11-12, 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morimoto US 7,024,553 in view of Spies et al. (hereinafter Spies) US 6,055,314 and in view of Trierger United States Letter Patent Number 6,226,750.

As per claims 4, 11 and 24:

The combination of Morimoto and Spies teaches all the subject matter as discussed above. Both references do not explicitly disclose a method wherein said key generator generates a first new encryption key; compares said new encryption key to the previous k encryption keys used in said network; and generates a second new encryption key if said first new encryption key matches any of said k previously used encryption keys.

Trierger in analogous art, however, discloses a method wherein said key generator generates a first new encryption key; (Col. 11, lines 30-32) compares said new encryption key to the previous k encryption keys used in said network; (Col. 11,

lines 39-41) and generates a second new encryption key if said first new encryption key matches any of said k previously used encryption keys. (Col. 11, lines 38-43)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Morimoto and Spies with Trieger to include wherein said key generator generates a first new encryption key; compares said new encryption key to the previous k encryption keys used in said network; and generates a second new encryption key if said first new encryption key matches any of said k previously used encryption keys. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Trieger (Col. 11, lines 38-39) in order to ensure the previous key is not reused.

As per claims 5, 12 and 25:

The combination of Morimoto, Spies and Trieger teaches all the subject matter as discussed above. In addition, Trieger further discloses a method wherein k is a user-defined number of previously used encryption keys. (Col. 11, lines 38-43)

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHEWAYE GELAGAY whose telephone number is (571)272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. G./  
Examiner, Art Unit 2437

/Emmanuel L. Moise/  
Supervisory Patent Examiner, Art Unit 2437